MAINTAINING A MILITARY EDGE OVER CHINA

RISKS OF INTERDEPENDENCE

America’s most senior military officers and civilian defense leaders in both parties have grown increasingly alarmed by China’s advancing military capabilities. Unclassified U.S. intelligence assessments describe the PLA as slowly but steadily transforming itself “from a defensive, inflexible ground-based force charged with domestic and peripheral security responsibilities to a joint, highly agile, expeditionary, and power-projecting arm of Chinese foreign policy that engages in military diplomacy and operations across the globe.” U.S. forces, by comparison, have deferred some of their own modernization programs and declined in readiness across many areas since 2001, partly due to a preoccupation with counterterrorism and counterinsurgency. Even after the Afghanistan withdrawal, America’s enormous and highly capable military remains spread thin across a number of global missions—whereas the PLA has been optimizing for a few key objectives in its local theater. Together, these trends have led the Pentagon to warn of a diminished “competitive edge” over China.

Technology plays a key part in China’s military catch-up. Beijing has made major strides in modernizing its conventional hardware and nuclear weapons systems—aided, at times, by cyber and traditional espionage. Looking ahead, many U.S. analysts are especially worried about the PLA’s incorporation of emerging digital technologies such as AI and quantum computing. China believes that AI, in particular, will eventually enable “intelligentized warfare”—a more rapid, precise, and dispersed form of combat intended to paralyze enemy forces and decisionmakers.
Because AI and so many other militarily relevant technologies are dual-use, the PLA seeks technical support from Chinese companies and universities under the banner of “military-civil fusion.” Seamless fusion remains more aspiration than reality; however, Beijing is working to break down bureaucratic barriers and enhance incentives for private support to the military. It also has many legal and extra-legal tools to compel such cooperation for high-priority military programs. This makes the U.S. defense establishment leery of technological cooperation between American and Chinese businesses or universities. The Pentagon fears that Beijing will leverage such links to acquire military-relevant technology, whether through licit means (such as joint ventures) or illicit means (like hacking).

**RISKS AND LIMITATIONS OF DEFENSIVE MEASURES**

The need to maintain a military edge over China offers powerful justification for U.S. technology controls. But what sort of controls can achieve American military needs at acceptable overall cost to the U.S. national interest? A narrowly tailored set of restrictions makes the most sense for several reasons. First, although AI and other emerging, dual-use technologies may someday become key factors in the U.S.-China military balance, that day is probably a long way off. The coming wave of military-technological advances will likely produce a marathon competition that lasts many years or even decades. This means the United States should prioritize the long-term sustainment of American innovative capacity rather than the short-term curtailment of Chinese military advances. Technology controls that durably set back PLA modernization would be worthwhile, but restrictions that degrade America’s own technology base while only briefly disrupting Chinese progress would be counterproductive.

It will likely take many years or even decades before AI and other emerging, dual-use technologies become key factors in the U.S.-China military balance.

To gauge the near-term role of AI in U.S.-China military competition, consider a potential confrontation in the Taiwan Strait occurring in the next few years—the central worry of today’s U.S. defense leaders. According to most analysts, the outcome of a Chinese incursion would likely hinge on such traditional factors as the PLA’s competence in amphibious assaults, the readiness of Taiwan’s defensive forces and the willpower of its civilian population and leaders, and the U.S. military’s regional force posture and rules of engagement. AI would certainly not be decisive. A recent analysis of Chinese military contracts found that, “like the United States, China’s most promising AI applications so far seem to be for back-office tasks like intelligence analysis and predictive maintenance.”

At what point will military AI become important enough to swing a battle between U.S. and Chinese forces? The National Security Commission on Artificial Intelligence—
the leading mainstream assessment—placed this risk “in the coming decades.” And how likely is it that Chinese AI would one day be sufficient to offset U.S. military advantages in other areas? The commission was appropriately cautious, simply noting that Beijing “believes” this could happen. DOD’s most recent public report on the Chinese military also hedged on whether, how, and when emerging technologies like AI or quantum computing might affect real-world combat. The report rightly gave more weight to less exotic developments, such as China’s ballistic and cruise missile advancements, its anti-satellite capabilities, its increasingly realistic joint exercises, and other modernization efforts. Of course, the era of AI warfare will come eventually and the U.S. military must work hard to prepare for it. But the longer this technology competition lasts, the less likely it is that U.S. restrictions will hold Chinese advances at bay.

Second, the Pentagon’s “competitive edge” concept is notably vague and open-ended, making it a poor guide for determining which technologies merit U.S. government restrictions. Nearly all technology has some military application, and the U.S. military sees itself “competing” with China in innumerable ways and places—from combat contingencies in the Indo-Pacific to steady-state information operations and defense diplomacy in Africa and Latin America. Controlling all the technologies relevant to such competition would mean a total amputation of U.S.-China tech ties—choking the American economy that funds defense spending, and degrading the U.S. innovation base that supports military capability development.

DOD has never actually called for full-scope decoupling; in fact, the DOD-aligned JASON group of scientific advisers has argued that international technical cooperation is vital to American interests. Yet U.S. military leaders have sometimes flirted with more restrictionist ideas—for example, generically opposing Americans’ involvement in the Chinese AI sector. Such ideas, if pursued to their logical conclusion, could lead to broad-based technological decoupling.

Finally, the U.S.-China rivalry is not just military in nature, and Washington will likely rely more on economic and diplomatic tools in the years to come. That is because the current U.S. military “competitive edge” over China, diminished as it is, probably cannot be sustained. China has natural geographic advantages in its home theater, whereas U.S. forces must operate costly and vulnerable expeditionary bases and logistics lines. China’s defense budget will probably keep growing faster than American spending, which is projected to stay flat or rise slowly in real terms. The technologically inferior PLA can close many existing gaps at a faster pace than the U.S. military can create new ones. And for many military scenarios, such as a Taiwan Strait confrontation, Beijing will be more invested in the outcome and more politically capable of absorbing losses than Washington.

Of course, the United States should take all reasonable measures to mitigate these military disadvantages. But a detailed study by the RAND Corporation found that “as long as
the Chinese economy continues to grow faster than that of the United States and Beijing continues to make military modernization a priority, the challenges facing U.S. military planners in Asia will grow more severe over time. This means that other tools of U.S. national power will be crucial for managing China’s rise—something Beijing itself appears to recognize. Thus, Washington should avoid technology restrictions that yield immediate yet modest military gains but inflict larger, longer-term economic and diplomatic costs on the United States.

**RECOMMENDED POLICIES AND PROCESSES**

The Defense Department must focus and prioritize its concerns about Chinese tech. Specifically, DOD should identify future PLA technology milestones that would tangibly change military outcomes over a concrete time horizon. This rigor would help federal regulators design more targeted technological controls that achieve military needs while minimizing harm to other national interests.

A good starting point would be DOD’s China-related defense planning scenarios—a classified set of priority missions that might include, for example, helping to defend and/or resupply Taiwan. For each planning scenario, DOD could seek to identify what potential new PLA technological capabilities would most significantly increase the likelihood of U.S. mission failure. The time horizon being considered would shape the nature of DOD’s analysis. DOD could make fairly concrete predictions about what technologies will matter most during the next five or ten years, because U.S. and Chinese operational concepts will not drastically change during that time and most key technologies either already exist or have been theorized. To assess military-critical technologies on a longer timeline, DOD would need to make more speculative predictions, such as how early-stage technologies may mature over decades, and what the American and Chinese militaries of the future will look and fight like. Proposed controls on early-stage technologies should therefore meet a higher threshold of criticality and undergo more rigorous vetting.

Although DOD has formidable internal expertise in offices such as the Strategic Intelligence and Analysis Cell, its assessments should draw generously from the insights of independent technologists, military analysts, and China experts to avoid myopia and groupthink. Existing channels for engaging outside experts, like the JASON group, may need to be expanded or supplemented to account for the difficulty of making long-term technology predictions and the need to consider implications for a wide range of U.S. interests beyond...
defense. The Intelligence Community should also provide an independent check on DOD’s assessments. Once military-critical technologies have been identified, intelligence analysts should assess the likelihood of the PLA actually acquiring these technologies and effectively fielding them over different time horizons. Analysts would also evaluate China’s relative dependence on foreign tech transfer, as opposed to its indigenous ability to develop the same technologies.

Regulators would then consider the efficacy of potential technology controls, and an interagency review led by the National Security Council (NSC) would evaluate second- and third-order impacts, such as economic and diplomatic implications. Interagency review has long been the norm for many kinds of technology controls. But given the growing importance of dual-use technology, private sector–led “spin-on” innovation, and globalized supply chains, the NSC should assess whether current deliberative processes are sufficiently comprehensive and inclusive.

**CASE STUDIES**

**Drone swarms.** Drone swarms are a potential example of militarily significant technology that might merit new U.S. technology restrictions. Many military analysts worry that large swarms of cheap, autonomous, self-coordinating drones could neutralize U.S. military advantages over China. They fear that China could deploy these drone swarms to overwhelm and destroy large, expensive, relatively immobile American assets like aircraft carriers. If that fear is well-grounded, then China’s development and successful fielding of this technology could swing the balance of a strategically consequential battle.

Still, U.S. technology controls would only make sense if they could be effective in protecting America’s military edge. China’s world-class commercial drone industry is mostly indigenous, reducing the U.S. government’s influence over Chinese advancements. In late 2020, the Trump administration added DJI, the global market leader in drones, to the Entity List based on human rights violations. David Benowitz, an industry analyst and former DJI official, identified several U.S.-origin parts that DJI would need to replace following this designation. Still, he predicted the move would not “severely impact” the company.

Swarming, an aspect of drone technology that remains in development, could have distinct chokepoints for U.S. controls to target. Key hardware components of drone swarms, like high-fidelity short-range communication equipment, might perhaps be controllable (assuming China does not already lead in these areas). Some software components, however—like computer vision algorithms—would be harder to control because they are intangible, under development by many international companies, and often based on openly published academic research.
Xiaomi. The final days of Trump’s presidency offered a vivid example of poorly designed technology controls, when DOD designated the consumer electronics giant Xiaomi as a “Communist Chinese Military Company.” This status, a forerunner of Biden's Non-SDN Chinese Military-Industrial Complex Companies List, would have prohibited Americans from investing in the company. DOD’s justification was shockingly thin. It highlighted Xiaomi’s plans to invest in 5G and AI—two broad, loosely defined technology areas that most global companies are pursuing—and the fact that Xiaomi was once publicly recognized by a Chinese ministry. Xiaomi later won a court injunction after a federal judge found the company did not meet the legal criteria for designation and DOD “could not identify any transfers of technology from Xiaomi to the PRC.” Biden has since reversed this designation and overhauled the underlying regulatory process, placing the Treasury Department in charge.

Broad technology categories like “AI,” “Big Data,” or “the Internet of Things” are not appropriate targets for military-related technology restrictions. They are too ubiquitous to control, and too generic to meaningfully assess for military impact. Unfortunately, the U.S. government does not always recognize this. The Commerce Department’s new ICTS supply chain rule requires special scrutiny for any China-related technology “integral to: (A) Artificial intelligence and machine learning; (B) Quantum key distribution; (C) Quantum computing; (D) Drones; (E) Autonomous systems; or (F) Advanced Robotics.” These are diverse and capacious categories. They can be a starting point for further analysis, but U.S. government decisionmaking must be far more granular.

Supercomputers. Supercomputers provide another case study that illustrates the complexity of U.S. efforts to control military-relevant technology. The U.S. government has long sought to prevent the Chinese military from acquiring powerful supercomputers due to their important role in advanced cryptography and in the design and development of nuclear weapons, missiles, and other military systems. For decades, Washington relied on export controls of finished supercomputers, permitting their sale to China only if they would not be used for military purposes. But U.S. restrictions have recently broadened. The United States now uses its Entity List to target entire Chinese organizations involved in supercomputing—restricting them from obtaining a wide range of U.S. components and other goods, not just supercomputers themselves.

Although these initial designations focused on organizations owned or controlled by the PLA, they have sprawled since 2015. Today the Entity List covers nearly all major players in the Chinese supercomputing ecosystem, including high-performance chip designers, supercomputer manufacturers, and supercomputer operators. According to the Commerce
Department, these organizations have varying ties to the PLA. Secretary of Commerce Gina Raimondo explained that “supercomputing capabilities are vital for the development of many—perhaps almost all—modern weapons and national security systems, such as nuclear weapons and hypersonic weapons.” But that is hardly all, or even most, of what some of these entities do. Like supercomputing organizations around the world, they also support biomedical research, weather forecasting, electric grid management, oil and gas exploration, and countless other benign activities.

On one level, this increasing use of the Entity List makes sense. China has transitioned from purchasing foreign supercomputers to building its own, so U.S. technology controls will be more effective if they target the latter process instead of the former. Yet the change in U.S. regulatory tools has also implied a subtle but important de facto shift in U.S. policy toward China’s technological development. Before, Washington specifically opposed Beijing’s military use of supercomputers. Now, it effectively opposes Chinese supercomputing as a whole—a general-purpose technology with innumerable civilian uses. The U.S. government has yet to publicly comment on this shift, which could have second- and third-order implications. It might stymie scientific cooperation on climate modeling, for example, or help motivate Beijing to restrict American access to some general purpose technology that China dominates. The Biden administration should carefully review its semiconductor restrictions to ensure that it has fully considered their implications beyond the military sphere.

**KEY OFFENSIVE POLICIES**

While senior defense leaders should continue to inform civilian regulators of the critical technologies they believe warrant government controls, other ways of maintaining the American military edge over China deserve more time and attention. First, DOD should accelerate its efforts to modernize and transform U.S. forces to counter the PLA. This work—which includes developing more survivable and cost-effective systems, becoming more adept at incorporating private sector innovations, designing new warfighting concepts for near-peer battle, and moving forces into and within the Indo-Pacific—has been underway since late in the Obama administration. However, it remains far from complete and faces enormous bureaucratic and congressional obstacles. The U.S. military edge over China will depend more on this task than on any other governmental effort, including technology restrictions.

Second, the Department of Defense and the Department of Homeland Security (DHS) should redouble their efforts to shore up cybersecurity and information security in the military and among defense

---

*The U.S. military edge over the PLA will depend more on the modernization and transformation of American forces than on technology restrictions targeting China.*
contractors specifically. The immediate priority would be to counter the most proven and most damaging Chinese intelligence collection techniques—namely, remote hacking, human agent recruitment, and open-source research. Although the Pentagon in recent years has significantly tightened the cybersecurity requirements in its procurement rules, the defense industrial base remains vulnerable.266
MAINTAINING A MILITARY EDGE OVER CHINA


241 The research also found that “U.S. companies are inadvertently powering Chinese military advances in AI” due to “loopholes and shortfalls in the export control system.” However, this problem is challenging to address and not cost-free, as discussed elsewhere. Ryan Fedasiuk, “We Spent a Year Investigating What the Chinese Army Is Buying. Here’s What We Learned,” Politico, November 10, 2021, https://www.politico.com/news/magazine/2021/11/10/chinese-army-ai-defense-contracts-520445.


250 For example, the Lowy Institute’s most recent Asia Power Index found that China is investing and gaining more in its international economic ties than in its defense capabilities and relationships. Hervé Lemahieu and Alyssa Leng, “Asia Power Index: Key Findings 2021,” Lowy Institute, 2021, https://power.lowyinstitute.org/downloads/lowy-institute-2021-asia-power-index-key-findings-report.pdf.

251 This example is hypothetical.


